nacro We change lives

Data protection and the use of criminal offence data for employment and education purposes

AUGUST 2018

PART ONE

BAN THE BOX: DATA PROTECTION AND THE USE OF CRIMINAL OFFENCE DATA FOR EMPLOYMENT AND EDUCATION PURPOSES

1. Background

The Rehabilitation of Offenders Act (ROA) allows most convictions and all cautions, reprimands and final warnings to be considered spent after a certain period. This period – known as the rehabilitation period – is determined by the sentence or disposal given, rather than by the type of offence. The ROA gives people with spent convictions, cautions, reprimands and final warnings the legal right not to disclose them when applying for most jobs and courses.

Most jobs and courses are covered by the ROA, but some are exempt. If a person applies for a job or course that is exempt from the ROA, the organisation is entitled to request details of spent and unspent convictions, cautions, reprimands and final warnings that are not protected. It is then entitled to take this information into account when determining the person's suitability for the role.

The Disclosure and Barring Service (DBS) provides a verification service in the form of a certificate that discloses criminal offence data. The level and type of data eligible for disclosure is determined by the nature of the role or course applied for. For roles and courses that are covered by the ROA, a criminal conviction certificate or basic check containing the prescribed details of all unspent criminal convictions is provided by the DBS on receipt of an application. An application for this certificate is made under s.112 Police Act 1997. An individual can apply for their own basic disclosure. An organisation that is registered with the DBS as a 'Responsible Organisation' can also apply.

For roles and courses that are exempt from the ROA, a criminal record certificate or DBS standard certificate disclosing spent and unspent convictions, cautions, reprimands and final warnings that are not protected can be obtained. An application is made under s.113A Police Act 1997 and is restricted to organisations, known as 'Registered Bodies', that are registered with the DBS. Individuals cannot apply for a copy of their own DBS certificate. For certain roles and courses that are exempt from the ROA, an application can be made under s.113B Police Act 1997 for a DBS enhanced certificate which may, in addition to the information that is disclosed on DBS standard certificate, include other information that the police feel is 'relevant' to the role applied for. If the role or course involves working in 'regulated activity' with adults or children, an additional check of the adults' and/or children's barred list can be conducted.

It is common practice for employers to ask all job applicants and volunteers to disclose criminal offence data as part of the recruitment process. Many organisations request this information at the job application stage. For roles that are covered by the ROA, the majority of organisations do not obtain basic checks to verify the criminal offence data that is provided to them by applicants, either during the recruitment process or after job offer. For roles that are exempt from the ROA, organisations generally obtain DBS standard or enhanced certificates for verification purposes after a provisional job offer has been made or the selected candidate has commenced employment.

The same applies to education providers, who very rarely conduct basic checks on prospective students. They can only lawfully undertake a DBS standard or enhanced check on prospective and existing students for courses that involve a voluntary or paid placement engaging in work that would be considered exempt from the ROA.

2. Data protection framework

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. Simultaneously, the Data Protection Act 1998 (DPA 98) was replaced by the Data Protection Act 2018 (DPA 18).

Previously criminal offence data was categorised as sensitive, personal data that could only be processed if certain conditions were met.

The term 'processing' applies to a comprehensive range of activities. It includes the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal.

Under GDPR, in order to process personal data about criminal convictions or offences, an organisation must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.

Article 10 applies to personal data relating to criminal convictions and offences, or related security measures. The concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under DPA 98.

In addition to having a lawful basis, an organisation must also satisfy one of the conditions found under Parts 1, 2, 3, of Schedule 1, DPA 18 and comply with additional safeguards set out in the Act. Even if an organisation has a condition for processing offence data, they can only keep a comprehensive register of criminal convictions if they are doing so in an official capacity.

Finally, and most importantly, when processing, storing and retaining criminal offence data an organisation has a duty to comply with the overarching principles of GDPR.

3. Data protection principles

The principles under the new data protection framework are broadly similar to the principles found in the Data Protection Act 1998 (DPA 98).

Below is an interpretation of the seven overarching principles found under GDPR, when applied to criminal offence data.

a. Lawfulness, fairness and transparency

An organisation must:

- Identify a 'lawful basis' for collecting and using criminal offence data
- Ensure that they do not do anything with the data in breach of any other laws
- Use this data in a way that is fair – this means they must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned
- Be clear, open and honest with people from the start about how they will use their data

b. Purpose limitation

An organisation must:

- Be clear about what their purposes for processing are from the start

- Record their purposes for processing criminal offence data as part of their documentation obligations and specify them in their privacy information for individuals
- Only use the data for a new purpose if this is compatible with their original purpose, they get consent, or they have a clear basis in law.

This principle is closely linked to the principle of the fairness, lawfulness and transparency. Being clear about why they are processing criminal offence data will help organisations to ensure that their processing is fair, lawful and transparent. If they use this data for unfair, unlawful or 'invisible' reasons, it is likely to be a breach of both principles.

c. Data minimisation

An organisation must ensure that the personal data they are processing is:

- Adequate – sufficient to properly fulfil their stated purpose
- Relevant – has a rational link to that purpose, and
- Limited to what is necessary – they do not hold more than they need for that purpose

For criminal offence data, it is particularly important for the organisation to make sure that they collect and retain only the minimum amount of information.

d. Accuracy

An organisation must:

- Take all reasonable steps to ensure that the criminal offence data they hold is not incorrect or misleading as to any matter of fact
- Keep the criminal offence data updated, although this will depend on what they are using it for
- Take reasonable steps to correct or erase incorrect or inaccurate criminal offence data as soon as possible
- Carefully consider any challenges to the accuracy of this data

e. Storage limitation

An organisation must:

- Not keep criminal offence data for longer than it is needed
- Be able to justify how long they keep criminal offence data for; this will depend on their purposes for holding the data
- Have a policy that sets out standard retention periods wherever possible, to comply with documentation requirements
- Periodically review the criminal offence data they hold to ensure that they are not in possession of spent or protected criminal offence data that is no longer relevant, or can not legally be taken into account for employment purposes, and erase it when they no longer need it

f. Integrity and confidentiality (security)

An organisation must ensure that they have appropriate security measures in place to protect the criminal offence data they hold.

g. Accountability

The accountability principle requires organisations to take responsibility for what they do with criminal offence data and how they comply with the other principles.

Organisations are responsible for, and must be able to demonstrate, compliance with the other principles. Organisations need to be proactive about data protection and evidence the steps they take to meet their obligations and protect people's rights. Good practice tools that the Information Commissioner's Office (ICO) has championed for a long time, such as privacy impact assessments and privacy by design, are now formally recognised and legally required in some circumstances.

4. Lawful basis

Under the GDPR, an organisation must have a valid lawful basis in order to process criminal offence data. There are six available lawful bases for processing. Most lawful bases require that processing is 'necessary'. If an organisation can reasonably achieve the same purpose without the processing, they won't have a lawful basis. The lawful basis must be determined prior to the processing and should be documented. The privacy notice should include the lawful basis for processing as well as the purposes of the processing.

The three bases that would appear most relevant for processing criminal offence data in an employment and education context are consent, public task and legitimate interests.

a. Consent

When obtaining criminal offence data organisations should:

- Check their consent practices and their existing consents – consents should be refreshed if they don't meet the GDPR standard
- Ensure a very clear and specific statement of consent is obtained in order for it to be considered explicit
- Keep their consent requests separate from other terms and conditions
- Be clear and concise
- Name any third-party controllers who will rely on the consent
- Make it easy for people to withdraw consent and tell them how
- Keep evidence of consent – who, when, how, and what you told people
- Keep consent under review and refresh it if anything changes
- Avoid making consent to processing a precondition of a service
- Take extra care to show that consent is freely given, and should avoid over-reliance on consent

The GDPR sets a high standard for consent. Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent when it comes to obtaining criminal offence data. Consent to process or retain the data may also be withdrawn by the individual at any time.

Organisations will therefore often be unable to rely on consent. If consent is difficult to show, organisations should look for a different lawful basis.

b. Public task

An organisation can rely on this lawful basis if they need to process personal data:

i) 'In the exercise of official authority' – this covers public functions and powers that are set out in law

ii) To perform a specific task in the public interest that is set out in law

It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest defined by the Freedom of Information Act 2000 (FOIA), the Freedom of Information Act (Scotland) 2002 and any authority or body specified by the Secretary of State in regulations. However, such an authority or body will only be considered 'public' when performing a task carried out in the public interest or in the exercise of official authority vested in it.

c. Legitimate interests

An organisation can rely on this lawful basis to process criminal offence data if:

- It is likely to be most appropriate where the organisation uses criminal offence data in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing
- They take on the extra responsibility for considering and protecting people's rights and interests
- The processing is necessary. If the organisation can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply

Legitimate interests is the most flexible lawful basis for processing and is probably the most appropriate basis for processing criminal offence data. Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

Organisations relying on this basis must:

- Balance their interests against the individual's. If the individual would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override the legitimate interests of the organisation

- Keep a record of the organisation's legitimate interests assessment (LIA) to help demonstrate compliance if required

- Include details of the organisation's legitimate interests in their privacy information

- Consider the following three stage test:

  i) **Purpose test:** is the organisation pursuing a legitimate interest?
  ii) **Necessity test:** is the processing necessary for that purpose?
  iii) **Balancing test:** do the individual's interests override the legitimate interest?

5. Criminal offence data – additional conditions

Once a lawful basis has been established, one of the conditions found under Parts 1, 2, 3, of Schedule 1, DPA 18 must be met.

For employment purposes, including voluntary work, the most relevant condition appears to be the **Part 1(1) Employment, social security and social protection.**

1(1) This condition is met if:
(a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject ***in connection with employment***, social security or social protection, and
(b) When the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this schedule).

For education purposes the conditions appear to be far more restrictive. Courses with a health and social care aspect that involve a placement may meet the **Health or social care condition 2 (2) d & e**.

2(1) This condition is met if the processing is necessary for health or social care purposes.
2(2) In this paragraph "health or social care purposes" means the purposes of—
(d) The provision of health care or treatment
(e) The provision of social care

Additionally, s. 184 (6) DPA 18 provides a broad definition of employment, which means that any other courses that involve paid employment, voluntary placements or on-the-job training will be covered by the employment condition outlined above. However, education providers may find it difficult to find a condition under which they can require students of other courses to make criminal record declarations.

6. Ban the Box – general principles

Ban the Box is a campaign that aims to create a fair opportunity for people with convictions to compete for jobs based on their skills and experience. The campaign calls for employers to:

- Remove the default tick box asking about criminal records from job application forms and move the declaration of criminal offence data to a later, more relevant stage of the recruitment process
- Ensure applicants are considered first on their skills, experience and ability to do the job before asking about criminal records

The campaign is currently in its fifth year with more than 100 employers signed up. The problem with the tick box approach is:

- It provides no opportunity to contextualise, explain circumstances or show progress since conviction
- It can make it difficult for candidates to get past the initial sift; criminal record declaration can become short-hand for 'bad' employee
- The very people who need to get into work may deselect due to the tick box
- Employers are missing out on committed and motivated individuals who can address their skills shortages

Given the reinforcement of data protection principles by the introduction of GDPR and DPA 18 the question is: Is there a requirement for organisations to 'ban the box' in order to comply with the requirements of the new data protection legal framework?

7. Ban the Box and data protection

Current employment and education practices where an individual is required to disclose criminal offence data at application stage may constitute a data protection breach for the following reasons:

a. Relying on consent as a lawful basis

Organisations that rely on consent to process criminal offence data at application stage will struggle to demonstrate that consent for processing the information is freely given by applicants. Having a criminal declaration on an application form imposes a condition on the applicant; namely that they must provide the requested information in order for their application to be considered.

Under GDPR, consent for processing criminal offence data can be withdrawn at any stage. However, in practical terms, an individual is precluded from withdrawing their consent to complete a criminal record declaration form on an application as to do so in most, if not all, instances will result in their application being rejected.

b. No legitimate interest – failing to meet the three-stage test

i) Purpose test: is the organisation pursuing a legitimate interest?

Organisations that require the disclosure of criminal offence data as part of the recruitment process, but who do not conduct any form of assessment of the criminal offence data that has been provided to them by a candidate and/or do not verify the information provided by way of a criminal record check, will struggle to demonstrate the purpose of requesting the information. Such an approach cannot be said to protect the organisation's interests in terms of safeguarding or complying with a legal or contractual obligation.

ii) Necessity test: is the processing necessary for that purpose?

For those organisations that can demonstrate a legitimate interest, requiring the disclosure of criminal offence data from individuals at the application stage is problematic as they are unlikely to verify the information until much later in the recruitment process. Therefore, criminal offence data obtained at this stage has little to no purpose with regards to protecting the organisation's interests e.g. safeguarding. Further, organisations rarely have a process in place at this stage of the recruitment process to assess the veracity of the criminal offence data and its relevance to the role.

It would not be practicable for most organisations to implement a criminal offence data assessment process and verification checks at application stage. Therefore, organisations will struggle to demonstrate that there is a **necessity** to obtain criminal offence data from all applicants at application stage.

iii) Balancing test: do the individual's interests override the legitimate interest?

It could be argued that in the absence of having an assessment and verification process at application stage, given the point raised above in respect of necessity, the interests of the applicants would override any legitimate interest the organisation may have as this would be limited in scope to those individuals that are being properly considered for the role. If the only criterion that is being assessed at application stage is skills, abilities and experience, disclosing criminal offence data would not provide any beneficial interest to the individual. If criminal offence data is being taken into account at application stage then this is likely to be for sifting purposes which could be considered discriminatory, adversely impacting the individual's interests.

c. Breach of data protection principles

- Having no formal criminal offence data assessment process and verification at application stage, and taking that information into account when making an employment decision without demonstrating and explaining the rationale behind that decision, could be considered **unfair processing, lack of transparency and lack of purpose (Principles A and B)**
- Asking all applicants to disclose criminal offence data when that information cannot be verified and can only truly become relevant and useful at a later stage of the recruitment process could be considered **gathering too much data (Principle C)**

8. Data protection good practice

The ICO's Employment Practices Code – although mainly relating to the principles contained with DPA 98 – can equally be applied to the principles introduced under GDPR and requirements of DPA 18. The guidance makes it clear that:

'A balance must be struck between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of organisations in deciding how best, within the law, to run their own businesses.'

In order to comply with data protection and to strike this balance we would advise organisations to:

- Assess whether the collection of criminal offence data is relevant to the recruitment process
- Remove any questions about criminal records that do not have to be asked at the initial application stage
- Ensure that the purpose of collecting criminal offence data is explained on the application form or surrounding documentation
- Ensure that the purpose of collection satisfies one of the data protection conditions
- Where the need to protect the organisation's business, customers, clients or others warrants the collection and verification of details of an applicant's criminal convictions, organisations in England and Wales should use only a disclosure from the DBS for this verification; organisations based in Northern Ireland can obtain a disclosure from Access NI, while organisations in Scotland can obtain a disclosure from Disclosure Scotland
- Do not attempt to obtain criminal offence data by forcing an applicant to use his/her subject access right or from sources other than the DBS
- Confine the obtaining of a disclosure of criminal offence, as far as practicable, to shortlisted applicants or those you intend to appoint

PART TWO

Is GDPR the game changer for Ban the Box?

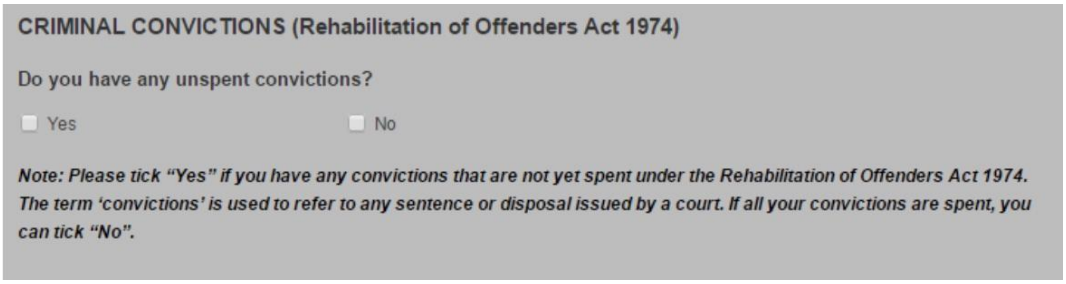
With UK unemployment at a record low, many of those who are currently unemployed and furthest away from the labour market are from disadvantaged groups (See Potential campaign).

At a time when employers across many sectors are competing to fill their skills gaps, we have both a societal and economic need for employers and recruiters to ensure that they remove all unnecessary barriers to filling their vacancies.

In light of the recent changes to data protection legislation (GDPR/DPA 2018), employers that require applicants to disclose their criminal record at the initial application stage should review their policies and processes to ensure they comply with GDPR requirements and are **fair to all candidates** regardless of their background. They need to minimise risks of discrimination by ensuring they do not have policies or practices that either explicitly or inadvertently put off otherwise suitable candidates with the right skills and abilities to do the job.

Nacro believes that the landmark changes to data protection legislation, together with the recent launch of the MOJ education and employment strategy and government plans to reform the Public Services (Social Value) Act 2013 – which will strengthen their commitment to awarding contracts based on social value, rather than just value for money – may be the final impetus needed for Ban the Box to be enshrined in law for all employers in the public and private sectors.

Consider the following example. This is a criminal record declaration used on an application form for a job in retail, but is typical of the type of criminal record declarations many organisations will have on their existing application forms:



CRIMINAL CONVICTIONS (Rehabilitation of Offenders Act 1974)

Do you have any unspent convictions?

☐ Yes ☐ No

Note: Please tick "Yes" if you have any convictions that are not yet spent under the Rehabilitation of Offenders Act 1974. The term 'convictions' is used to refer to any sentence or disposal issued by a court. If all your convictions are spent, you can tick "No".

- It could be argued that asking about criminal records in this instance does not pass the **necessity test** for collection of criminal record data required under GDPR/DPA 2018. The role itself is not subject to a criminal record check and relies entirely upon self-declaration. The employer cannot demonstrate that they have met the **purpose test** in this instance.

- Simply asking a Yes/No question or providing the candidate with a couple of lines to give full details about their criminal record does not give the candidate a **fair or adequate** opportunity to provide any level of useful detail to the employer that would enable them to make an informed, evidence-based assessment about their suitability for the role. The employer is unlikely to be in a position to demonstrate the rationale behind any decision to reject the candidate at this stage based on their criminal record, particularly when 11 million people in England and Wales have one.

- The question about the candidate's criminal record on this application form serves no **beneficial purpose** for either the employer or candidate. If used in the sifting process, it can result in the exclusion of suitable candidates as there is not an adequate opportunity for the candidate to provide any context in relation to their criminal record, the circumstances in their life that led to their offending behaviour, or to demonstrate how they have moved on from their past mistakes.

- During this initial sift of applications the employer does not have enough information to establish the relevance of any conviction disclosed by the candidate for the role applied for, so they cannot demonstrate that they have complied with GDPR **fairness requirements.** This leaves them at risk of facing claims of discrimination. They cannot demonstrate that they have considered the other risk assessment principles: nature and seriousness of offence(s), length of time since first and last offence, age at time of offending etc. Both GDPR and the DBS Code of Practice require an organisation to have a recruitment of ex-offenders policy considering these factors.

- It is unlikely that the employer has a system in place to determine or verify the accuracy of any conviction disclosed by the candidate for the role applied for. The candidate may have over-disclosed or under-disclosed.

- The information contained on the application form is not adequately protected. It is considered sensitive information, yet it can potentially be viewed by any member of staff who is in receipt of the application form, anyone involved in the sifting or other aspects of the recruitment process and maybe even anyone who has access to staff files, if the person were to be recruited. It is **not transparent** how the employer will use this information within the recruitment process or that they will store it **securely and confidentially** should the candidate be recruited, as application forms might be stored for the length of the employment relationship (potentially without a review period in place). The employer in this instance is unlikely to be able to demonstrate that they are **handling the candidate's personal data properly.**

- Requiring this information at this stage can clearly be viewed as **intrusive and excessive**. Only a limited number of candidates will be shortlisted for interview. The application form should be designed in such a way that the candidate is able to provide sufficient information that demonstrates whether they have the necessary skills or qualifications to warrant moving forward to the next stage of the recruitment process, without requiring the disclosure of a criminal record that cannot be accurately verified at this stage.

- Following this, an employer asking about criminal records on the initial application could also be in breach of other laws and may be at risk of claims of indirect discrimination by a candidate who has the necessary skills and abilities for the role, but feels that they have been treated unfairly due to an arbitrary approach being applied to the declaration of their criminal record.

- It is well known that many people with criminal records come from disadvantaged backgrounds (See Potential Campaign). The Lammy Review and Freshfields' research highlighted that people from BAME backgrounds are disproportionately represented in the criminal justice system. Government statistics show that care leavers are also disproportionately represented.

- Recently, in the High Court, several women successfully argued that the disclosure of their convictions for being forced to work in the sex trade many years ago was disproportionate and a breach of their Article 8 Human Rights, the right to a private life.

- Ban the Box has gained momentum in parts of the public sector:

  - The Ministry of Justice's education and employment strategy includes implementing Ban the Box throughout the public sector, including across all local authorities

  - Bristol City Council is the first to publicly sign up as a Ban the Box employer

  - The government has also developed a pilot entry route into the Civil Service for ex-offenders that Nacro has been involved with called Going Forward Into Employment (GFIE)

  - The Civil Service has banned the box across 97% of all roles. It would be hard for an employer in the example above to argue that their environment is more sensitive than government roles, particularly as they are relying upon self-declaration

- Even if the role was subject to a standard or enhanced DBS check, the employer cannot argue that they need to gather the information at this stage in the recruitment process. They would be gathering other more critical information such as qualifications and experience on the application form which would determine whether the applicant should proceed to the next stage of the process – all of which would need to be verified at a later stage.

- Employers should be mindful that alongside banning the box, it is important to have in place a transparent ex-offender policy and process that demonstrates how they will consider any criminal record disclosed and the rationale for any decision made.

- For all the reasons mentioned in this briefing and many more, Nacro believes that all employers across the public, private and voluntary sector are now required to Ban the Box.

Briefing produced by Nacro with input from DHA